# Exhibit A

# FISCH SIGLER LLP

5301 Wisconsin Avenue NW | Fourth Floor | Washington, DC 20015 USA

February 13, 2020

**R. William Sigler**
**Partner**
Bill.Sigler@FischLLP.com
Direct: +1.202.362.3520
Main:  +1.202.362.3500

**VIA EMAIL**

Mr. Vincent Rubino, Esq.
Brown Rudnick LLP
7 Times Square
New York, New York 10036
vrubino@brownrudnick.com

Re:   *Longhorn HD LLC v. Juniper Networks, Inc.*
Case No. 2:19-cv-00385-JRG (E.D. Tex.),
**SUBJECT TO FRE 408**

Dear Vincent:

Thank you again for the courtesy of extending the deadline to respond to Longhorn's complaint. I write because our study of the patents-in-suit and the complaint's allegations indicate that this action should proceed no further.

As an initial matter, Juniper intends to file a motion to transfer the case to the Northern District of California under 28 U.S.C. § 1404(a) should the case go forward. As explained in the attached draft motion and declaration, five times, in cases brought by other plaintiffs, the Eastern District has granted similar Juniper motions. This case presents many of the same factors that those five prior decisions relied on, including the location of the evidence and relevant witnesses in the Northern District of California.

Juniper also intends to file petitions for *inter parties* review on all five patents-in-suit should the case go forward. These petitions will rely on prior art references that we have located after an initial search that predate the priority date for the patents-in-suit and read on the claims. Copies of Juniper's draft petitions for the '778 and '846 patents are enclosed for your consideration.

Additionally, Juniper's study of the patents-in-suit and Longhorn's allegations shows that the accused products do not infringe. The complaint reveals a fundamental misunderstanding of the accused products and the relevant technology. The following are four non-exhaustive examples of this.

1. The complaint alleges that Juniper infringes the '732 patent because the "[t]he SRX unit receives requests for communication with the server from entities originating outside the network and establishes communication between the two entities." But this is incorrect. Instead, the SRX series implements the Dynamic Host Configuration Protocol (DHCP) in response to requests for communications, which the patentee explicitly stated its invention did not cover during prosecution. Specifically, to
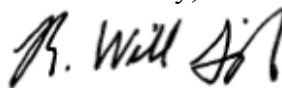
**FISCH SIGLER** LLP

- 2 -

overcome the prior art reference U.S. Patent No. 6,122,276 ("Boe"), the patentee described Boe as "making reference to DHCP." The patentee then stated that its "invention is the opposite scenario of *Boe et al*," and thus did not cover the use of DHCP. (*See* Jan. 16, 2002 Response to Office Action at 14.) Given this disclaimer, Federal Circuit precedent precludes Longhorn from accusing Juniper of infringing through the use of DHCP. *See, e.g., Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1323 (Fed. Cir. 2003).

2. The '778 patent requires "a second object directory server installed in the second intranet to dynamically install a service proxy in the second dynamic proxy server when the service is provided in the second Intranet." But the SRX device firewall serves as a middleman for decryption purposes with the necessary services preinstalled in response to a service request. Thus, the SRX doesn't "dynamically install a service proxy" as the patent requires.

3. The '846 patent is directed to a method for monitoring and analyzing network traffic packets capable of classifying "anomalous behavior as an event selected from the group consisting of a network fault, a change in network performance and a network attack." But the accused Juniper systems don't classify network traffic in this manner. Instead, when determining if a given file is malware, Juniper's threat prevention system returns a verdict score between 0 and 1, with a threshold for indicating likelihood of malware in an inspected file. In other words, Juniper's threat prevention system only looks for a single file type and determines the percentile chance of whether the analyzed file is malware. It does not—as the patent claims require—classify suspect network traffic into different categories.

4. For the '790 patent, the complaint alleges that "a user of a mobile client is uniquely identified to the mobile VPN system, for example, a device Media Access Control ("MAC") address." And for the '421 patent, the complaint further states that "the Accused Products associate at least one selected process, such as, for example, HTTP or FTP, with at least one network address, such as, for example, a MAC address." But the SRX series products don't use MAC addresses for these purposes. Instead, they rely on usernames for the identification of users and matching of policies.

In light of the facts outlined here, dismissal of the complaint is appropriate. I am available to discuss an amicable wrap-up to the case before we proceed with filing our motion to transfer and petitions for *inter partes* review. Thank you.

Sincerely,

Bill Sigler